CUSTOM APPLICATION BEHAVIOURAL SECURITY MONITORING USING SIEM

AGENDA FOR TODAY

- Introduction
- Problem Statement
- Application Security Monitoring Process
- Q & A

WHO ARE WE?

Himanshu Tonk
Junior Manager , Cyber Risk Services
Deloitte Netherlands
Expertise: Security Monitoring , Threat Hunting

Prithvi Bhat
Junior Manager , Cyber Risk Services
Deloitte Netherlands
Expertise: Security Monitoring, Risk assessments.

DUE TO VARIED PRIORITIES AND FOCUS ON CORE BUSINESS ORGANISATIONS OFTEN STRUGGLE WITH SECURITY MONITORING OF CROWN JEWEL.

- Organisations struggle to identify relevant threats and setting up security monitoring/detection.
- Alignment of security requirements to business objectives.
- Availability of usable data that can be converted into tangible use-cases.
- Expertise in building advanced monitoring content.

APPLICATION SECURITY MONITORING

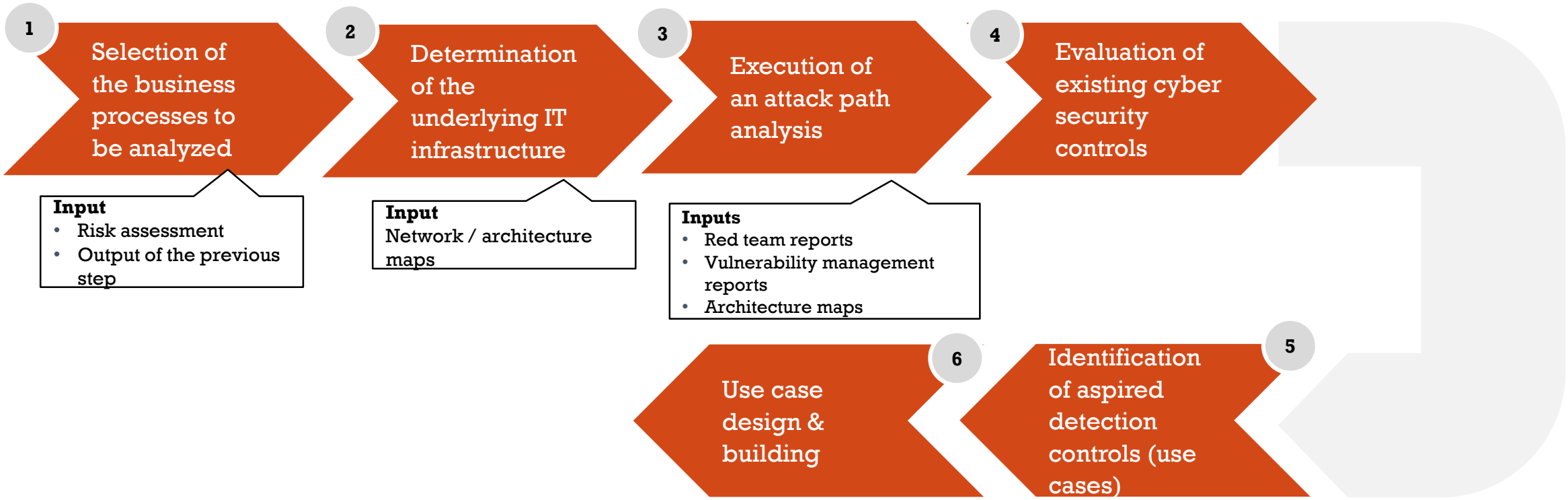
Five step Process

Identification & Threat Modelling of Critical Application	Onboarding	Implementation	Documentation	Maintenance
• Selection of application for monitoring • Threat modelling to uncover the underlying threats	• Connecting & ingesting security data in to monitoring platform	• Security content development • Alerting & follow-up	• Purpose & design document • Playbooks	• Tuning of the security content based on feedback & knowledge gained

IDENTIFICATION AND RATING OF POTENTIAL APPLICATIONS BY SCORING THEM ALONG THREE FACTORS

Actual risk coverage	Speed of implementation	Visibility within Organization
Risk mitigated, based on the threats, exposure and potential impact.	Ease and speed of onboarding the application and its use-cases.	Ability to show the added business value of security monitoring.

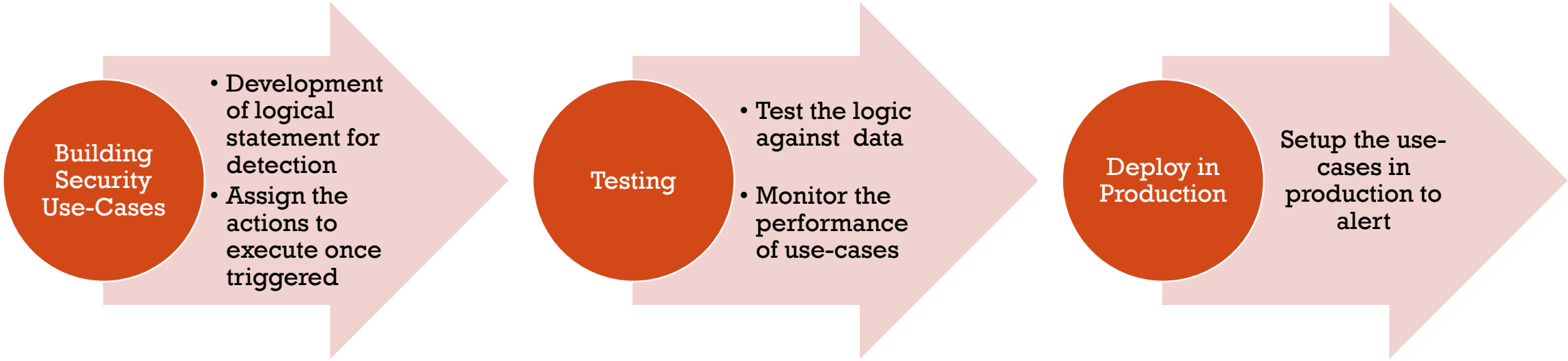
ONBOARDING APPLICATIONS IS DONE USING A STANDARDIZED THREAT MODELING AND USE CASE DESIGN PROCESS



ONBOARDING OF IDENTIFIED APPLICATION/S TO THE MONITORING PLATFORM

Application & technology research	Categorize log events	Sample log deep-dive	Estimate feasibility and efficiency	Connect data
• Read up on technology stack if not yet familiar. • Retrieve relevant documentation and gain an understanding what is possible within the tech stack.	• Structure received sample logs, categorize available events and gain understanding of types of events available. • Use previous research to identify and add events not present in sample.	• Deep-dive into log sources to identify events that are relevant to the identified use-cases.	• Make initial estimate of performance impact on SIEM and the application itself. • Make initial estimate whether tuning the amount of alerts to acceptable and usable levels is possible.	• Define path to the monitoring platform and organize access. • Test run data connections and connect data to the platform in the final form.

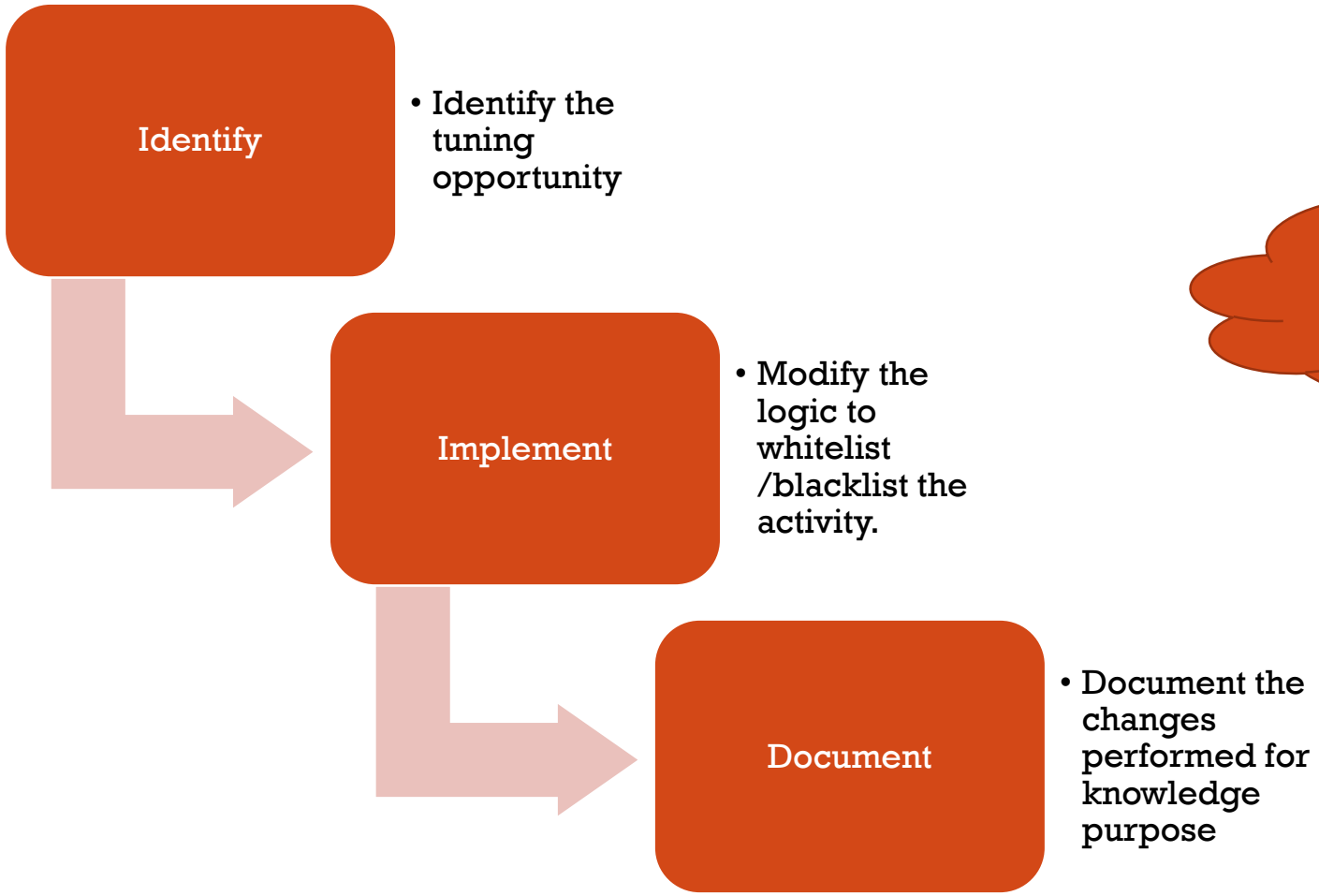
IMPLEMENTATION OF DESIGNED USE-CASES IN MONITORING PLATFORM



DOCUMENTATION

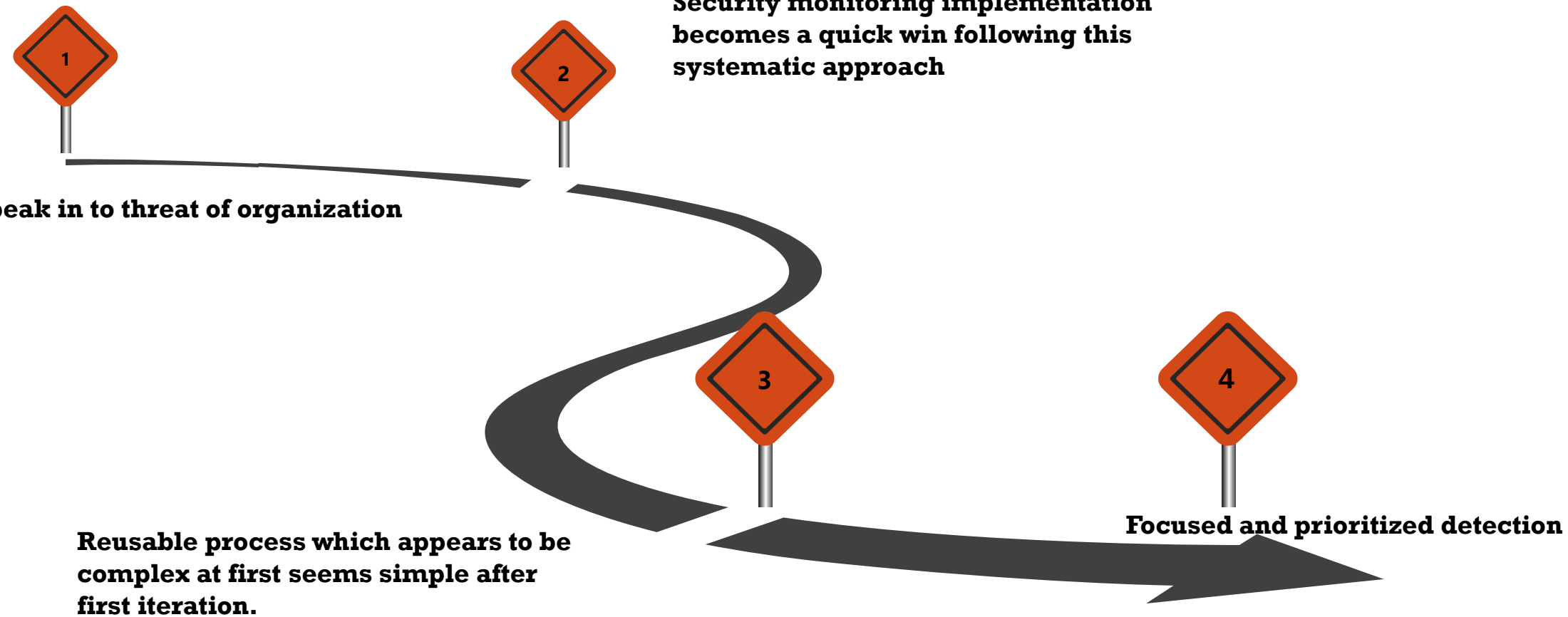
Purpose & Design Statement	• Goal of the use-case and monitored threat • Technical design of the use-case
Playbooks	• Investigation steps to triage the alert • Should include relevant stakeholders and type of notification

MAINTENANCE OF USE-CASES



Regular tuning is the key to effective use-cases

CONCLUSIONS



Sneak peak in to threat of organization

Security monitoring implementation becomes a quick win following this systematic approach

Reusable process which appears to be complex at first seems simple after first iteration.

Focused and prioritized detection

?????????

Please don't ask tough questions